Applying for and Interoperating with the Federal Bridge Certification Authority

Purpose: This white paper briefly describes what an agency needs to do to apply for cross-certification and interoperate its PKI with the production Federal Bridge Certification Authority (FBCA).

Where additional information and assistance can be obtained: The Operational Authority for the FBCA is the General Services Administration (GSA), and the governing body for FBCA use is the Federal PKI Policy Authority. Information concerning the FBCA, including detailed technical data on the products employed by the FBCA, can be found on the GSA web page at http://gsa.gov/<tbd>, and information on the Federal PKI Policy Authority, including the application form which an agency will use to apply for interoperability with the FBCA, the FBCA Certificate Policy and Certificate Profile, can be found at http://<tbd>. Additionally, assistance in completing the application form can be obtained through the Federal PKI Policy Authority as set forth on their web page. Further, a glossary of relevant terms used in this white paper can be found in the Internet Engineering Task Force Request for Comment number 2828 at http://www.ietf.org/rfc/rfc2828.txt. Finally, technical assistance in dealing with any of the matters discussed in this white paper can be obtained by contacting GSA, the Federal PKI Steering Committee (http://gits-sec.treas.gov), or the Federal PKI Policy Authority at the URLs cited above.

Distinction between the prototype and production FBCA: The Operational Authority operates a prototype FBCA and a production FBCA. The former is used for testing purposes (including testing the addition of CA products before they are included in the production FBCA), whereas the latter is used to effect interagency PKI interoperability. Interoperability with the former, for testing purposes, may be permitted by the Operational Authority, whereas interoperation with the latter, even at the "test" level of assurance, requires the approval of the Federal PKI Policy Authority. Wherever the term "FBCA" is employed in this paper, it is assumed to mean the production FBCA unless otherwise indicated.

Costs for interoperation with the FBCA: Interoperation with the FBCA, including the application process therefor, is at no cost to the applicant through Fiscal Year 2001. Beyond that time, the Federal PKI Policy Authority (for processing applications) and the FBCA Operational Authority (for interoperating with the FBCA, and using the FBCA directory) shall prescribe what fees, if any, apply.

Discussion: Using the production FBCA to effect interagency PKI interoperability entails completing six steps.

First, an agency must have an operational or planned PKI with a CA (called an Agency "Principal CA") which they wish to cross-certify with the FBCA, one or more Certificate Policies (CP), a Certification Practice Statement for the Principal CA, and a description of the directory structure they use to support their PKI (especially with respect to how they control and manage the namespace for the certificates they issue).

Second, an agency must apply to the Federal PKI Policy Authority to obtain a certificate from the FBCA to the agency's Principal CA. This application is done using a form supplied by the Federal PKI Policy Authority (available on its web site, http://<tbd>), which must be filled in by the applicant agency and signed by a senior official of the agency (as established on the form). The application contains how the agency proposes to map the certificate levels of assurance present in the agency's CP to the levels expressed in the FBCA CP, and how the agency's certificate profile conforms to the Federal Certificate Profile (available at the Federal PKI Policy Authority web site cited above). The application also describes how the applicant agency's PKI has been independently audited to ensure conformance by the applicant to its own CP and CPS.

Third, the Federal PKI Policy Authority will evaluate the application and either accept the policy mapping proposed by the applicant or propose an alternative mapping. If the applicant accepts the alternative mapping, the Federal PKI Policy Authority will execute with the applicant a Memorandum of Agreement (MOA) which reflects the respective responsibilities of the Federal PKI Policy Authority and the agency along with the policy mappings. Among other things, the MOA and the documents it includes (such as the FBCA Certificate Profile and its references) describe: (a) how the main fields and the extensions in the certificate issued by the FBCA to the agency Principal CA, and the cross-certificate from the Principal CA to the FBCA, will be populated; (b) how those fields will be populated in the certificates issued within the agency's PKI; and (c) how Certificate Revocation Lists issued by the FBCA and agency CAs will be populated. The MOA also addresses how the agency will interoperate its directory or directories with the Federal PKI (which may include the FBCA directory, or other agency directories directly). (Note: The issue of directory interoperability is separately addressed in more detail later in this document.) A draft "notional" MOA will be made available on the Federal PKI Policy Authority web site; the draft MOA will be tailored to the specific terms negotiated between the Federal PKI Policy Authority and the applicant. This negotiation process may be completed quickly or may require substantial effort, depending upon the nature of the proposed mapping and other factors. After the MOA is signed by the parties, the cross-certificates are then issued.

Fourth, the agency must then actually effect directory interoperability with the Federal PKI. Testing thus far has successfully employed LDAP queries to a local Directory System Agent with X.500 chaining between directories. It is expected that LDAP with referrals between directories will also work but that has not yet been tested.

Fifth, the agency must ensure that the certificates it issues within its own PKI are populated in conformance with the Federal Certificate Profile, which describes how extensions are to be populated and interpreted. The agency must also ensure that CRLs issued within its own PKI are also populated in accordance with the Federal Certificate profile.

Finally, for the agency to be able to employ the FBCA certificates, it must ensure that client software (for the application or applications it wishes to PKI-enable) has the ability

to create and process certificate trust paths. This may be done using commercial off the shelf software as-is, or with plug-ins supplied by vendors to commercial client software, or by developing custom software specifically for that purpose. Ensuring that the client software properly conforms to the X.509 processing requirements, when it is installed and periodically thereafter, is vitally important for agency users to be assured that they are only accepting externally-issued certificates they wish to accept for transactions.

However, it should be emphasized that the Federal PKI Policy Authority does not require the agency to have such client software before authorizing issuance of a certificate from the FBCA to the agency Principal CA. Indeed, if an agency only performs steps one through five, certificates it issues can be accepted by other agencies for transactions. For it to accept certificates issued by other agencies, the agency must also perform the final step.

Further, it should be noted that where the applicant agency has a test or prototype PKI, the agency may wish to interoperate that PKI with the prototype FBCA before the MOA is finalized and the cross-certificates between the agency production PKI and the production FBCA are issued. As cited previously, interoperability with the prototype FBCA only requires agreement by the FBCA Operational Authority. Interoperation between a test or prototype PKI and the production FBCA is only expected to be done at the "test" level of assurance set forth in the FBCA Certificate Policy.

Technical details and assistance in dealing with each of the elements discussed in this paper (above and below) can be found either on the Federal PKI Policy Authority web page, the FBCA Operational Authority web site, or by contacting either organization as described on their respective web sites. Each organization has resources available to assist applicants in interoperating with the FBCA and ensuring that the applicant's PKI can constructively employ FBCA certificates. Information available on the web sites or from those organizations includes:

- FBCA Directory Information Tree
- Required directory schema
- Supported algorithms, their parameters, and associated Object Identifiers
- Directory IP addresses and port numbers
- Certificate and CRL requirements extracted from the Federal Certificate Profile
- Formats/protocols for exchanging public key information for cross-certification
- Known configuration parameters for Agency Principal CAs and for directory systems for products supported by the FBCA
- List of commonly encountered problems (and their resolution) when attempting FBCA interoperability

Specific issues for agency consideration: The remainder of this white paper discusses specific issues which an agency must consider in deciding how best to interoperate with the FBCA, while ensuring that the agency is able to protect its interests appropriately.

1. *Developing a Proper Certificate Policy*: An essential part of any PKI is a Certificate Policy (CP) describing the nature of the certificates issued by the Certification Authorities which the agency PKI comprises. This should be one of the first steps that an agency takes in developing a PKI. The CP must employ the standard IETF PKIX RFC 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" format, which is the format employed by the FBCA CP. The PKIX format is available at http://www.rfc-editor.org/rfc/rfc2527.txt. The FBCA CP is available on the Federal PKI Policy Authority web page, http://<tbd>. Each CP has a unique Object Identifier (OID) which is expressed in certificates issued under that CP; obtaining an OID is discussed further below.

2. *Registering Certificate Policy Object Identifier (OID) and Name Space*: Each agency Certificate Policy must have an associated OID registered under the International Standards Organization Object Identifier scheme. If the agency Certificate Policy has not already been issued an OID, the agency may obtain one from NIST through http://csrc.nist.gov/csor/. Additionally, obtaining an appropriate Directory Information Tree namespace (an "OU=") requires the agency to register with GSA <cite specific office of URL> if that has not previously been done by the agency.

3. *Enabling Client Software to use the FBCA*: For agency relying party client software to be able to create and process trust paths, the software must be able to discover cross-certificates and Certificate Revocation Lists (or Certification Authority Revocation Lists, which are CRLs for certificates issued to CAs). This means that the client software must do more than what has been required of such software in the past; that is, it must do more than just validate a signature on a certificate or on a document, it must create what are called "trust paths" of certificates that demonstrate a topological connectivity between the two interoperating CAs. Some PKI vendors offer this capability through plug-ins supplied for different applications programs (e.g., e-mail clients); this capability is available intrinsically in the Windows operating system for Microsoft CAs, and soon will be available for trust paths involving external, non-Microsoft CAs. In any event, it is essential that for the capability of the FBCA to be used, that is, for one agency to be able to trust certificates issued by another agency using the FBCA, the relying party client software must be able to create and process trust paths for this purpose. This function may also be done at the server level in order to reduce the burden on the client.

4. *Effecting Agency Directory Interoperability*: Where is the information needed to create and process trust paths held? Typically, it can be found in agency directories. Thus, PKI interoperability – the ability to create and process trust paths as cited above – boils down to finding this information and then processing it. To accomplish the first step ("finding the information"), the relying party client software makes requests of directory servers. Such requests may employ different protocols, such as LDAP, DAP, or proprietary mechanisms. Additionally, if the directory system agent local to the relying party does not have the information required, either it needs to obtain that information (using X.500 chaining) or it needs to provide the client with an indication concerning where the information can be located (LDAP referral) – and the client needs to know what to do with such a knowledge reference. NIST is developing a Directory Profile

(available at http://<tbd>) that provides a common framework within which client software can work to discover this information. If an agency's directory structure conforms to this framework, the agency should have increased confidence that client software will be able to discover the information needed for trust path creation and processing.

5. *Processing Trust Paths Properly*: Once a trust path is created, the client software must process it in accordance with X.509 in order to ensure that the relying party is not exposed to unacceptable transitive trust or other conditions that proper implementation of X.509 guards against. Achieving this requires that the relying party agency ensure that the client software is properly enabled and configured.

6. *Limiting Transitive Trust*: In a cross-certified model, it is important that entities who are cross-certified be able to describe with sufficient specificity whom they wish to trust, and (perhaps) whom they wish not to trust. For example, if one CA is cross-certified with another and only wishes to trust that CA, then a vulnerability could be created if that second CA itself cross-certifies with a third CA without notifying the first CA. Fortunately, X.509 (and implementations under the IETF PKIX) provides for several mechanisms which the first agency may employ to protect its interests, and vice versa. These techniques can be generalized to use of the FBCA as set forth below.

a. The certificate issued by the first CA to the second CA may express, in a certificate extension called "nameConstraints," which parts of the directory tree it wishes to trust or distrust. This is done by using the "permitted subtree" and "excluded subtree" elements. For example, if the first CA is owned by the Treasury Department and the second by the Department of Commerce, were Treasury only desiring to trust Commerce but no other CAs that Commerce may be separately cross-certified with, then Treasury would state in the nameConstraints extension of the certificate it issued to Commerce that the permitted subtree is "C=US, O=U.S. Government, OU=Commerce". This means that any certificate trust path containing external (to Treasury) certificates which are not contained in that subtree, would fail to validate (assuming the client software properly implements the X.509 processing rules).

Carrying this example further in the FBCA context, where both Treasury and Commerce are cross-certified with the FBCA, the certificate issued by Treasury to the FBCA would express in the nameConstraints extension that only the FBCA and Commerce domains are to be trusted. If Treasury desires to trust additional agencies, they too may be recited. Alternatively, if Treasury desires to trust all who are cross-certified with the FBCA without enumeration, the extension can be left blank.

As cited earlier, trust relationships can also be expressed by excluding domains. For example, Treasury could leave the "permitted subtree" entry blank (so it trusts all domains cross-certified with the FBCA), but then populate the "excluded subtree" entry with those domains it specifically desires NOT to trust. In that case, only the cited domains would fail to be trusted.

b. Certificates issued by the FBCA to an agency will always place in the "permitted subtree" element of nameConstraints the X.500 DIT occupied by that agency. Thus, the certificate issued by the FBCA to Treasury would express (in the "permitted subtree" element) only "C=US, O=U.S. Government, OU=Treasury".

Note that the certificate issued by the FBCA to an agency is used in trust path creation by other agencies, whereas the certificate issued to the FBCA by an agency is used in trust path creation by that agency. This means that such certificates will contain different contents in the nameConstraints extension. Moreover, it means that when an agency wishes to adjust whom it wishes to trust, that agency may revoke the certificate it issued to the FBCA and issue a new certificate containing the new description.